The Consultative Committee for Space Data Systems

Draft Recommendation for Space Data System Practices

SYMMETRIC ENCRYPTION

DRAFT RECOMMENDED PRACTICE

CCSDS 353.0-R-1

RED BOOK

October 2008

The Consultative Committee for Space Data Systems

Draft Recommendation for Space Data System Practices

SYMMETRIC ENCRYPTION

DRAFT RECOMMENDED PRACTICE

CCSDS 353.0-R-1

RED BOOK

October 2008

AUTHORITY

Issue:	Red Book, Issue 1
Date:	October 2008
Location:	Not Applicable

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in the *Procedures Manual for the Consultative Committee for Space Data Systems*, and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

STATEMENT OF INTENT

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF INTENT:)

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

PREFACE

This document is a draft CCSDS Recommended Practice. Its draft status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document's technical content.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 353.0-R-1	Symmetric Encryption, Draft Recommended Practice, Issue 1	October 2008	Current draft

CONTENTS

Section Page

1 INTRODUCTION.. 1-1

1.1 PURPOSE OF THIS RECOMMENDED PRACTICE 1-1
1.2 SCOPE 1-1
1.3 APPLICABILITY 1-1
1.4 RATIONALE 1-2
1.5 DOCUMENT STRUCTURE 1-2
1.6 REFERENCES 1-4

2 OVERVIEW 2-1

2.1 BACKGROUND 2-1
2.2 ALGORITHM SELECTION RATIONALE 2-2

3 ALGORITHM DESCRIPTION 3-1

4 SECURITY 4-1

4.1 INTRODUCTION 4-1
4.2 SECURITY CONCERNS WITH RESPECT TO THIS DOCUMENT 4-1
4.3 POTENTIAL THREATS AND ATTACK SCENARIOS 4-1
4.4 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY 4-1

ANNEX A INFORMATIVE REFERENCES (INFORMATIVE) A-1

Figure

3-1 Counter Mode 3-2
3-2 GCM Authenticated Encryption Function 3-3

1 INTRODUCTION

1.1 PURPOSE OF THIS RECOMMENDED PRACTICE

This Recommended Practice provides the basis for the use of a standard symmetric block-cipher encryption algorithm for civilian space missions. This Recommended Practice does not specify how, when, or where encryption should be implemented or used. Those specifics are left to the individual mission planners based on the mission security requirements and the results of the mission threat/risk vulnerability analysis. However, by using a standard algorithm, use of high-quality cryptography is ensured, the potential rewards of economies of scale by the ability to buy off-the-shelf products is enabled, and there is the potential for interoperability among missions using the same algorithm.

1.2 SCOPE

The symmetric encryption algorithm described in this document is recommended for use on all civilian space missions with a requirement for information confidentiality (e.g., data, voice, video). The algorithm may be employed on any or all mission communications links such as the forward space link (e.g., telecommand), the return space link (e.g., telemetry, science data) as well as over the ground data network. It could even be used to ensure confidentiality of stored data (e.g., 'data at rest') if there is a requirement to do so.

A symmetric algorithm assumes that all communicating entities possess a shared secret (i.e., a cryptographic key) which enables them both to encrypt and decrypt information shared among them. The manner in which the shared secret is distributed and managed is left for individual Agencies or missions to decide upon pending the development of a CCSDS Recommended Standard or Practice for key distribution and management. It should be noted that key management is not within the scope of this document.

1.3 APPLICABILITY

1.3.1 APPLICABILITY OF THIS RECOMMENDED PRACTICE

This Recommended Practice is applicable to all civilian space missions with a requirement for information confidentiality.

1.3.2 LIMITS OF APPLICABILITY

While the use of encryption is encouraged for all missions with an information confidentiality requirement, the results of a threat/risk analysis and the realities of schedule/cost drivers may reduce or eliminate its need on a mission-by-mission basis.

1.4 RATIONALE

Traditionally, security mechanisms have not been employed on civilian space missions. However, in recognizing the increased threat there has been a steady migration towards the integration of security services and mechanisms. For example, ground network infrastructures typically make use of 'controlled' or 'protected' networks. Nevertheless, while there may be confidentiality concerns regarding telecommands, telemetry, or science payload data, they are still, for the most part, transmitted over radio frequency (RF) channels in the clear. This practice needs to change as the threat environment becomes more hostile.

A CCSDS Recommended Practice for a symmetric encryption algorithm is necessary because of the increasing interconnection of ground networks; the movement towards 'joy-sticking' of instruments by principal investigators; the decreasing costs for hardware, potentially allowing cheap 'rogue' ground stations to be established; and national trends towards enhancing mission security. Such an algorithm establishes a common denominator among all missions for implementing confidentiality services.

1.5 DOCUMENT STRUCTURE

1.5.1 DOCUMENT ORGANIZATION

Four sections and one annex make up this document. Section 1 provides introductory information, definitions, nomenclature, and normative references. Section 2 provides background and rationale for choice of the algorithm. Section 3 describes the algorithm. Section 4 discusses security considerations related to use of symmetric encryption on the space link. Annex A provides informative references.

1.5.2 DEFINITIONS

Controlled Network: A network that enforces a security policy.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Ciphertext: Encrypted data.

Data Integrity: Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Denial of Service: Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. Such actions include any action that causes unauthorized destruction, modification, or delay of service.

Plaintext: Unencrypted data.

Residual Risk: The portion of risk that remains after security measures have been applied.

Risk: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact.

NOTE – Risk is the loss potential that exists as the result of threat and vulnerability pairs. It is a combination of the likelihood of an attack (from a threat source) and the likelihood that a threat occurrence will result in an adverse impact (e.g., denial of service, loss of confidentiality or integrity), and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk.

Risk Analysis: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

Security Policy: The set of laws, rules, and practices that regulate how information is managed, protected, and distributed.

NOTE – A security policy may be written at many different levels of abstraction. For example, a corporate security policy is the set of laws, rules, and practices within a user organization; a system security policy defines the rules and practices within a specific system; and a technical security policy regulates the use of hardware, software, and firmware of a system or product.

Threat: Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Threat Agent: A method used to exploit a vulnerability in a system, operation, or facility.

Threat Analysis: The examination of all actions and events that might adversely affect a system or operation.

Threat Assessment: Formal description and evaluation of threat to a system.

Vulnerability: Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy.

Vulnerability Analysis: The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Vulnerability Assessment: A measurement of vulnerability, which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

1.5.3 NOMENCLATURE

The following conventions apply throughout this Recommended Practice:

a) the words ‘shall’ and ‘must’ imply a binding and verifiable specification;

b) the word ‘should’ implies an optional, but desirable, specification;

c) the word ‘may’ implies an optional specification;

d) the words ‘is’, ‘are’, and ‘will’ imply statements of fact.

1.6 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this Recommended Practice. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Recommended Practice are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS documents.

[1] *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Special Publication 197. Gaithersburg, Maryland: NIST, 2001. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[2] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. National Institute of Standards and Technology Special Publication 800-38A. Gaithersburg, Maryland: NIST, 2001. <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>

[3] R. Housley. *Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)*. RFC 3686. Reston, Virginia: ISOC, January 2004. <http://www.ietf.org/rfc/rfc3686.txt>

[4] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. National Institute of Standards and Technology Special Publication 800-38D. Gaithersburg, Maryland: NIST, November 2007. <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>

[5] J. Viega and D. McGrew. *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*. RFC 4106. Reston, Virginia: ISOC, June 2005. <http://www.ietf.org/rfc/rfc4106.txt>

NOTE – Annex A contains informative references.

2 OVERVIEW

2.1 BACKGROUND

Confidentiality is defined as the *assurance that information is not disclosed to unauthorized entities or processes*. In other words, those who are not unauthorized are prevented from obtaining information. Confidentiality is accomplished by various mechanisms which prevent access to information: physical locks, guards, or gates. For communications systems, there are essentially two mechanisms: (1) transmission through a physically protected medium (e.g., wire encased in alarmed conduit) and (2) cryptography.

For the CCSDS community, the means by which information confidentiality must be performed is by cryptography. In civilian space missions, confidentiality may be employed to ensure non-disclosure of information as it traverses the ground network, as it is transmitted between the ground and the spacecraft, between the spacecraft and the ground, or even on-board a spacecraft.

A ground network may support numerous, simultaneous missions with many support personnel. Likewise, a ground station may support multiple missions, and several spacecraft might use the same communications frequencies. A single spacecraft might support instruments from various universities, agencies, or countries. All of these separate entities may have confidentiality concerns and may not allow their data or commands to be obtained or intermixed with others.

For human-crewed missions there are concerns regarding the confidentiality of medical information conveyed on-board, across the space link, and over ground communications infrastructure. Similarly, private communications between human crew members and their families, such as voice and email, must also be afforded confidentiality.

An encryption algorithm provides the basis on which confidentiality services can be implemented. Regardless of where or how the confidentiality services are applied, an encryption algorithm must be employed. As is illustrated in the CCSDS document entitled *The Application of CCSDS Protocols to Secure Systems*, (CCSDS 350.0-G-2, reference [A1]), there are multiple locations within the space communications layering model where an encryption algorithm can be employed. As is pointed out in reference [A1], there is no *single* right answer for positioning and employing encryption. Depending on the system, encryption may be implemented in an application (e.g., TLS/SSL, reference [A3]). It might be employed above the network layer as with SCPS-SP (reference [A4]) or IPsec (references [A5] and [A6]). It may be employed at the link layer or even at the physical layer (e.g., 'bulk encryption'). Or it may be employed simultaneously at multiple layers if that is advantageous to the system (e.g., at both the network and application layers).

While a multitude of encryption algorithms are available, both those requiring a license and those in the public domain, it is in the best interests of the CCSDS community to employ a modern, strong, well-analyzed public-domain encryption algorithm. The use of a public-domain algorithm eliminates the need to pay license, patent, or royalty fees. The use of a well-analyzed algorithm means that good, strong, secure cryptography will be employed.

2.2 ALGORITHM SELECTION RATIONALE

The Rijndael algorithm was selected as the Advanced Encryption Standard (AES) after a lengthy, open, international competition for a symmetric algorithm replacement for the 30+ year old Data Encryption Standard (DES). The algorithm was invented by Joan Daemen from Banksys/PWI and Vincent Rijmen from ESAT-COSIC, both in Belgium. It is available world-wide on a royalty-free basis. It is not covered by any legal restrictions or patents.

With many algorithms submitted to the competition, a thorough analysis was performed in an international forum resulting in five AES finalist algorithms: Rijndael, Twofish, Serpent, RC6, and Mars (see reference [A7]). No glaring cryptographic problems or differences were found among the five finalists, but in multiple implementation tests, Rijndael had the best performance in both hardware and software and subsequently was chosen as the standard algorithm.

The CCSDS Security Working Group performed an Encryption Algorithm Survey (reference [A8]) which examined thirteen algorithms ranging from DES and triple DES, the five AES finalists, the GSM/UMTS algorithms, as well as several other miscellaneous algorithms.

While a wide variety of algorithms were examined, the most widely studied and analyzed by the international cryptographic community are the five AES finalists. As a result, based on the original AES selection criteria, it appears to be in CCSDS's best interest also to adopt AES/Rijndael as its **recommended best practice** for symmetric encryption as specified in FIPS PUB 197 (reference [1]) with modes of operation described in NIST Special Publication 800-38A (reference [2]).

3 ALGORITHM DESCRIPTION

In order to achieve a minimum baseline among all CCSDS missions, the use of the Advanced Encryption Standard (reference [1]) algorithm using the Counter Mode of operation is **recommended**. The AES algorithm is specified in the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 197 (reference [1]). The Counter Mode of operation is specified in NIST Special Publication 800-38A (reference [2]). It is further described in the Internet Engineering Task Force (IETF) RFC 3686 (reference [3]).

AES is a publicly available algorithm with no licensing or patent restrictions. It is a modern, strong algorithm that has been deeply analyzed by the international cryptographic community. It is very efficient regardless of whether it is implemented in hardware or software.

AES is key agile and supports key sizes of 128-bits, 192-bits, or 256-bits. The CCSDS **recommended practice** is to use, as a minimum, a 128-bit key, but larger key sizes **may be used** for stronger security.

AES is a symmetric, block-cipher algorithm operating over a 128-bit block. The algorithm assumes a 128-bit plaintext input block which results in the output of 128-bits of ciphertext. In cases where the input is smaller than 128 bits, the input block must be padded to 128 bits unless the Counter Mode of operation is employed (see below).

As is stated in NIST Special Publication 800-38A (reference [2]), five modes of operation are defined for AES:

– Cipher Block Chaining (CBC);

– Electronic Code Book (ECB);

– Cipher Feedback (CFB);

– Output Feedback (OFB); and

– Counter (CTR).

At a minimum, the CCSDS **recommended practice** is to follow the IETF recommendation for use of AES with Internet Protocol Security (IPsec) and use of the Counter Mode as described in RFC 3686 (reference [3]). An illustration of Counter Mode is provided in figure 3-1.

Counter mode is a very efficient mode of operation. It differs from the other modes because the data to be encrypted is not run through the AES algorithm. Rather, a counter which has been combined with a cipher key is used as the starting input to the algorithm, which in turn produces 128-bit random key blocks. The output bits are XORed with the plaintext data to produce the output cipher blocks. Counter mode has a nice feature that reduces overhead by not requiring padding of partial blocks, a requirement in all other modes. If the last block of plaintext is not 128-bits, only the number of bits remaining are XORed with the produced key bits, and all the other key bits are discarded.

Also notable for the CCSDS community, counter mode operations can be pipelined. Because each block is independent, the encryption process does not have to be performed in a serial manner, taking output from one block as input to another. This translates into increased algorithmic performance with the assumption of CPU capabilities available to perform parallelized functions.

CTR mode requires the generation of a counter which does not have to be secret but must never repeat while a key is being used. If a counter is repeated then the confidentiality of the blocks encrypted under that counter may be compromised. In order to ensure the selection of a unique counter, an incrementing function should be used from an initial counter. The initial counter must be chosen to ensure uniqueness across all blocks encrypted under a given key. A random set of bits may be used as the initial counter. Alternatively, a message nonce may be chosen and incorporated into every counter block. The specific methods of choosing an initial counter block and generating subsequent counter blocks is described in reference [2], appendix B, page 18.

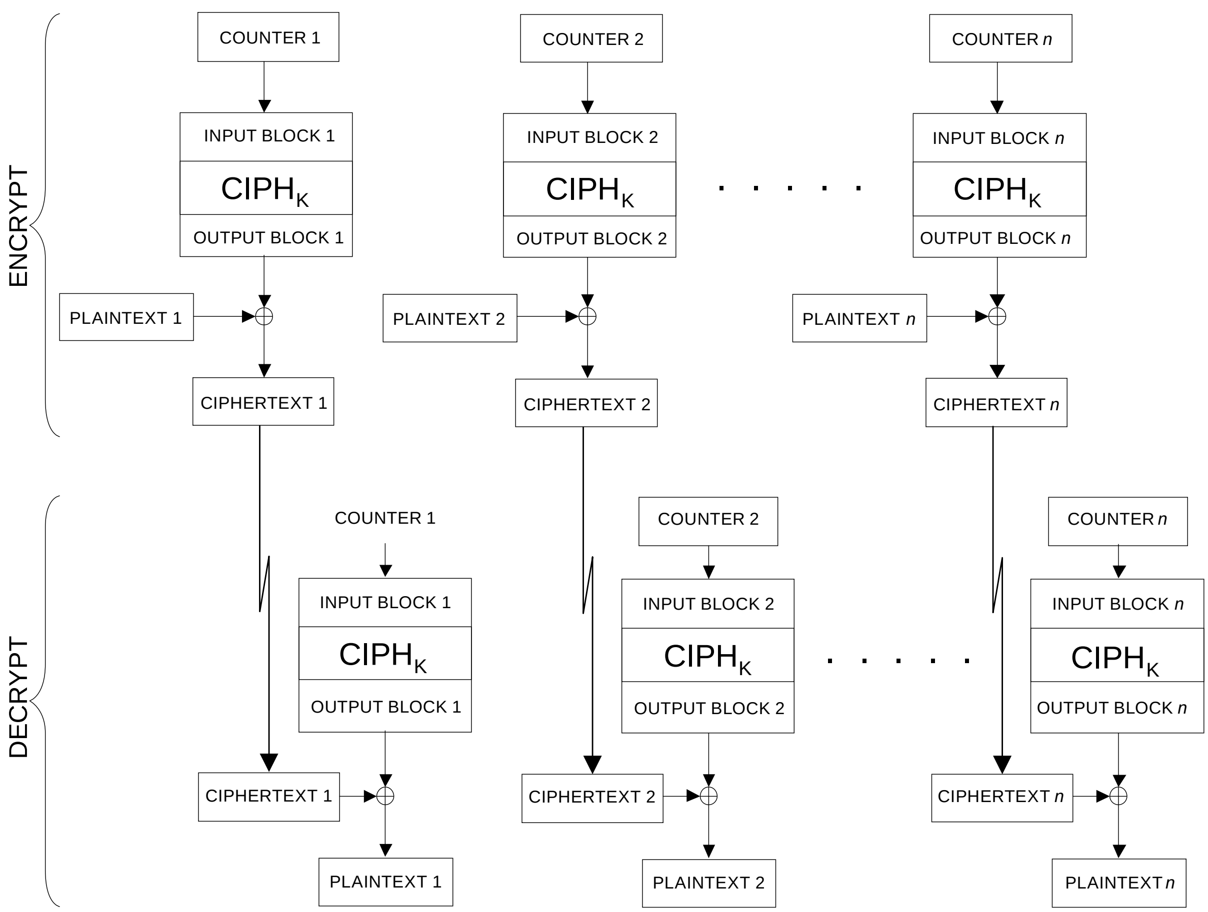

Figure 3-1: Counter Mode[1]

---

[1] *Source*: NIST Special Publication 800-38a (reference [2]), Figure 5.

While AES in counter mode operation is **recommended**, the cryptographic community has recognized that often data encryption without data origin authentication results in degraded overall security. As a result, several additional counter modes of operation that provide both encryption and data origin authentication have been specified. These modes are called Authenticated Encryption with Associated Data (AEAD).

AEAD modes include Offset Codebook (OCB), Counter with CBC-MAC (CCM), EAX, Carter-Wegman + Counter (CWC), and Galois/Counter (GCM). CCM is the mandatory mode used for wireless security in the IEEE 802.11i. OCB was originally proposed as the mandatory IEEE 802.11i mode, but is now optional. EAX (which has no acronym expansion) was proposed as a simpler replacement for CCM. CWC is a combination of counter mode with the efficient polynomial Carter-Wegman message authentication code. GCM was designed as an improvement over CWC. To provide authentication, CWC uses 127-bit integer multiplications, which are more operation-intensive than AES itself.

GCM, unlike most of the other AEAD modes, can provide very high-speed authenticated encryption in hardware as well as in software. It can also be parallelized and pipelined, methods that can be very advantageous in the space community. Unlike CWC, GCM's authentication uses binary field multiplication that can be implemented with great efficiency. GCM is specified in NIST Special Publication 800-38D (reference [4]) as well as in IETF RFC 4106 (reference [5]). An illustration of GCM is provided in figure 3-2 below. If encryption with data origin authentication is a desirable feature for a system, CCSDS **recommends** that GCM as specified in reference [4] and reference [5] be used.

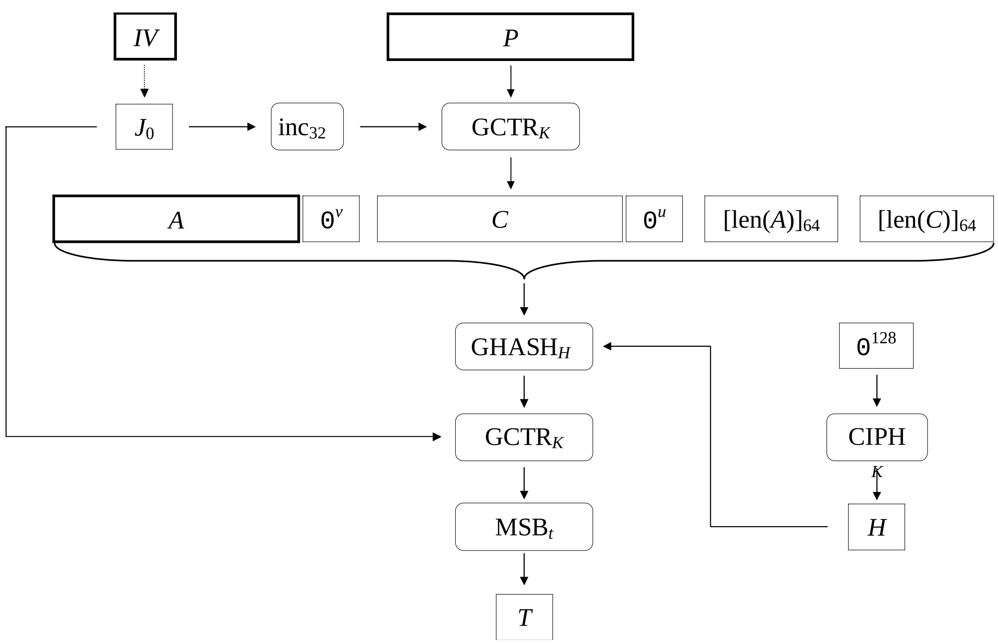

Figure 3-2: GCM Authenticated Encryption Function[2]

[2] *Source*: NIST Special Publication 800-38D (reference [4]), Figure 3.

4 SECURITY

4.1 INTRODUCTION

This section discusses the various aspects of security with respect to symmetric encryption and its use in the space environment. Encryption is based on the use of a cipher algorithm. Encryption provides the mechanism by which the information is made opaque. The 'plaintext' data is input to the algorithm and the resulting output is transformed into 'ciphertext' which, without the encryption key, is unreadable to maintain its confidentiality.

4.2 SECURITY CONCERNS WITH RESPECT TO THIS DOCUMENT

The entirety of this document is security related. It discusses a security mechanism, symmetric encryption, which is used to provide confidentiality of transmitted data. Encryption provides a means to prevent unauthorized disclosure of information. That is, if the information were not encrypted, a casual observer or an active attacker would be able to obtain the information.

4.3 POTENTIAL THREATS AND ATTACK SCENARIOS

If information's confidentiality is not protected using a mechanism such as encryption, it may be disclosed to unauthorized entities. In many cases this disclosure would not matter, but there are cases where it could result in the loss of proprietary data, loss of sensitive data, or loss of privacy data (e.g., human-crewed mission medical information). The information could be obtained by, for example, an eavesdropper listening to an RF transmission, a tap on a landline, or an unauthorized agency insider examining network traffic.

4.4 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

The unauthorized disclosure of this information could result, at worst, in total mission loss. For example, if spacecraft commands were disclosed to unauthorized entities, unauthorized commands could be sent to the spacecraft (e.g., performing an unauthorized thruster burn could result in the loss of a mission). It might result in the distribution of information to unauthorized entities when it had been agreed that principal investigators would have exclusive use of the information for a given time. It might also result in the disclosure of information which could have been for sale rather than given away (e.g., high resolution Earth observation imagery).

ANNEX A

INFORMATIVE REFERENCES

(INFORMATIVE)

[A1] *The Application of CCSDS Protocols to Secure Systems*. Report Concerning Space Data System Standards, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006.

[A2] [RFC]S. Frankel, R. Glenn, and R. Glenn. *The AES-CBC Cipher Algorithm and Its Use with IPsec*. RFC 3602. Reston, Virginia: ISOC, September 2003. <http://www.ietf.org/rfc/rfc3602.txt>

[A3] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol*. RFC 4346. Version 1.1. Reston, Virginia: ISOC, April 2006. <http://www.ietf.org/rfc/rfc4346.txt>

[A4] *Space Communications Protocol Specification (SCPS)—Security Protocol (SCPS-SP)*. Recommendation for Space Data System Standards, CCSDS 713.5-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

[A5] S. Kent and K. Seo. *Security Architecture for the Internet Protocol*. RFC 4301. Reston, Virginia: ISOC, December 2005. <http://www.ietf.org/rfc/rfc4301.txt>

[A6] S. Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303. Reston, Virginia: ISOC, December 2005. <http://www.ietf.org/rfc/rfc4303.txt>

[A7] [DEV]James Nechvatal, et al. “Report on the Development of the Advanced Encryption Standard - AES.” *Journal of Research of the National Institute of Standards and Technology* 103, no. 3 (May-June, 2001): 511–577. <http://nvl.nist.gov/pub/nistpubs/jres/106/3/j63nec.pdf>

[A8] *Encryption Algorithm Trade Survey*. Report Concerning Space Data System Standards, CCSDS 350.2-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, March 2008.

[A9] *PKCS #1 v2.1: RSA Cryptography Standard*. Bedford, Massachusetts: RSA Laboratories, June 2002. <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>

[A10] *PKCS #3: Diffie-Hellman Key-Agreement Standard*. Revised ed. Bedford, Massachusetts: RSA Laboratories, November 1993. <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-3.doc>

[A11] *Glossary of INFOSEC and INFOSEC Related Terms*. Compiled by Corey D. Schou. Pocatello, Idaho: Idaho State U Simplot Decision Support Center, 1996.

NOTE – Normative references are listed in 1.6.